



THREAT INTELLIGENCE
REPORT

TRXDrop Wallet Drainer Panel

TRON/Solana Angel Drainer reseller deploying fake TRX airdrop pages with forced signing loops

PUBLISHED

March 08, 2026

THREAT TYPE

Crypto Wallet Drainer

CLASSIFICATION

TLP:CLEAR

SEVERITY:
HIGH

PHISHDESTROY RESEARCH DIVISION • [HTTPS://PHISHDESTROY.IO](https://phishdestroy.io) • REPORT ID: PD-TRXDROP-2026-03-08

15+

DOMAINS

TRON/SOL

CHAINS

30 TRX

COMMISSION

10+

WALLETS TARGETED

Executive Summary

The TRXDrop Wallet Drainer Panel is a TRON/Solana wallet drainer operated by an Angel Drainer reseller. It utilizes fake TRX airdrop pages to deceive users and drain their TRX and USDT funds. The panel is currently active and has been linked to at least 15 domains.

The operation is managed by a threat actor using the Telegram handle `@STN1RAWbIaFLiH`. The panel has not yet reported any victim connections or approvals, indicating it may be newly deployed or inactive.

Threat Actor Profile

TELEGRAM HANDLE	ID	REGISTRATION DATE	ROLE
@STN1RAWbIaFLiH	6823931109	~December 2023	Panel support/operator

Known infrastructure connections include domains such as `trxdrop.live` and `trump-drop.world`.

Technical Infrastructure

COMPONENT	DETAILS
Frontend	React SPA (Create React App)
Backend	Node.js / Express
Auth	JWT HS256
CDN	N/A
Hosting	Unknown

API endpoints include `POST /api/auth/login`, `GET /api/user/profile`, and `POST /api/buildTransactions`.

Panel sections include Dashboard, TRON, Configurations, Solana, News, Profile, Hosting, and Support.

Attack Chain / Scam Flow

- Victim lands on fake TRX airdrop page.
- Page loads anti-debug protections and encrypted config.

3. Victim clicks Connect Wallet and sees a spoofed Trust Wallet modal.
4. Wallet connection is routed through WalletConnect or deeplinks.
5. Backend builds malicious transactions via `/api/buildTransactions`.
6. Victim sees fake "Receive 10,000 TRX (\$2,200)" message.
7. Victim signs transaction with up to 50 forced retries.
8. Signed transaction sent to backend via `/api/sendTransaction`.
9. TRX and USDT drained from wallet (minimum \$10 or 5 TRX).
0. 30 TRX auto-commission sent to operator.
1. Telegram notification sent to operator.

Indicators of Compromise

DOMAIN		STATUS
trxdrop.live		Active
trump-drop.world		Active
IP		ORG/COUNTRY
WALLET ADDRESS		CHAIN
TRAGn9E6hbTiQrYG5V4sk1gNv3JawHSxak		TRON
TELEGRAM ACTOR		ID
@STNlRAWbIaFLiH		6823931109

Victim Impact

GEOGRAPHIC REGION	IMPACT
-------------------	--------

Financial impact includes a minimum drain of \$10 or 5 TRX per victim. Promo code analysis is not available.

MITRE ATT&CK Mapping

TACTIC	TECHNIQUE ID	TECHNIQUE NAME	EVIDENCE
--------	--------------	----------------	----------

Countermeasures

- End users should verify wallet connections and avoid suspicious airdrop offers.
- SOC teams should monitor for domains and IPs associated with TRXDrop.
- Registrars should investigate and potentially suspend domains linked to the scam.
- Law enforcement should track financial transactions to identify operators.
- Use the [PhishDestroy free domain scanner](#) for domain risk assessment.
- Refer to the [DestroyList open-source blocklist](#) for known malicious domains.

References

- [PhishDestroy threat intelligence platform](#)
- [Free domain risk scanner](#)
- [DestroyList community-maintained blocklist](#)
- [ScamIntelLogs evidence archive](#)

Evidence Screenshots

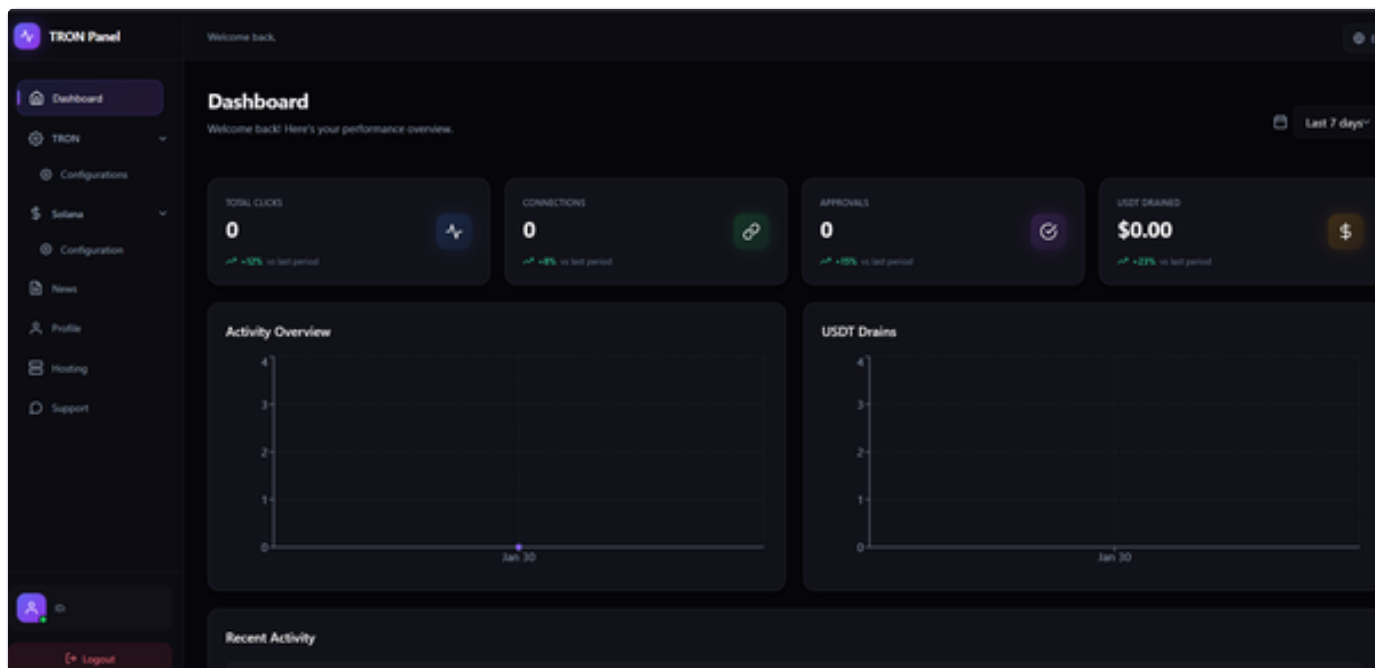


Figure 1: Panel/infrastructure screenshot captured during investigation

Create Configuration

Configuration Name ⓘ

My Configuration

\$ Transaction Settings ▲

Minimum Balance (\$) ⓘ

10

🛡️🔒 Force Approval Mode ▲

☐ 🔒 Enable Force Approval ⓘ

Only request Approval (no transfer). Funds will be drained via AutoDrain when balance >= \$1000

🔔 Notifications ▲

Telegram Chat ID ⓘ

123456789

Telegram Bot Token ⓘ

123456:ABC-DEF...

Figure 2: Panel/infrastructure screenshot captured during investigation

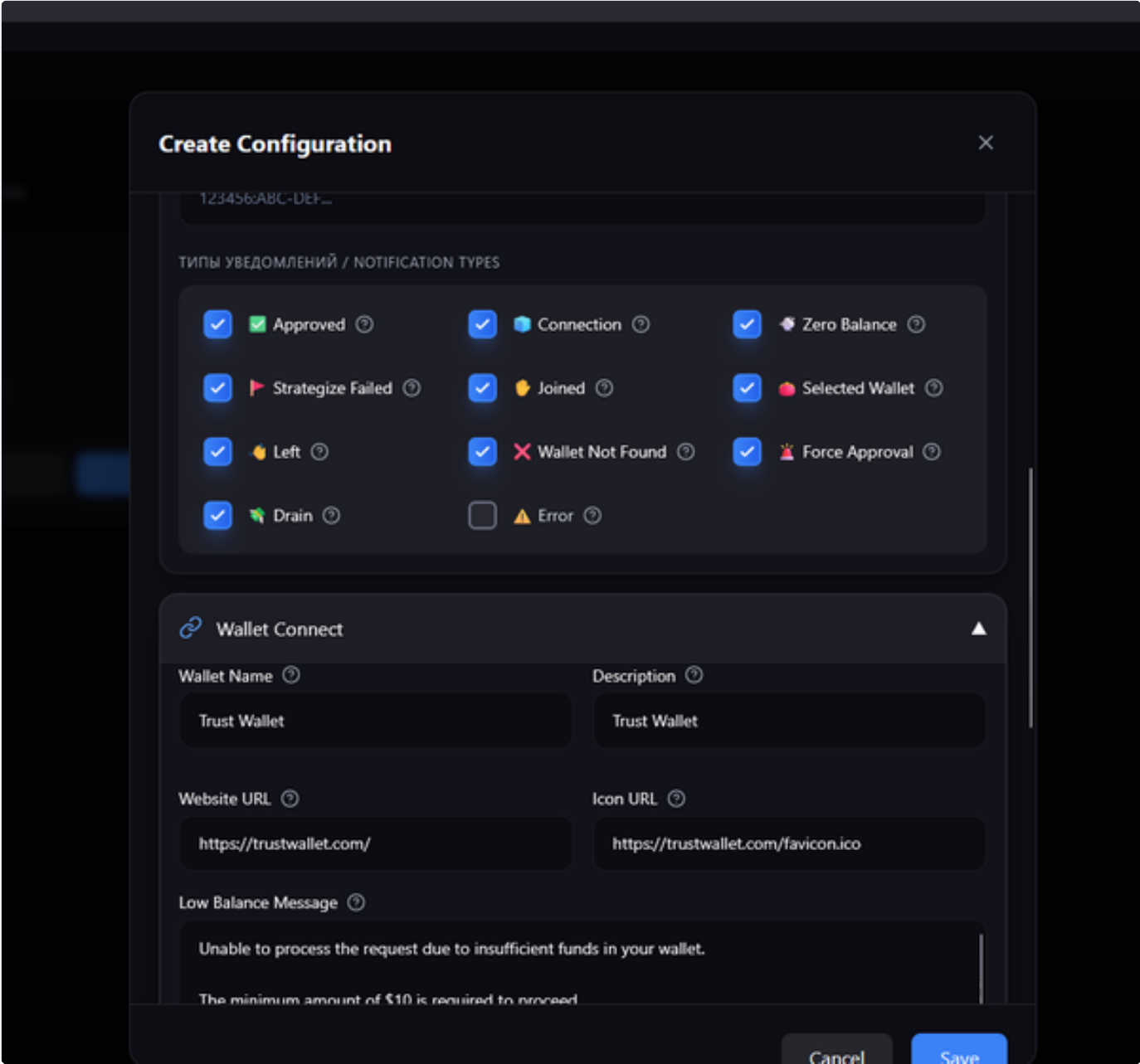


Figure 3: Panel/infrastructure screenshot captured during investigation

[Download IOCs \(CSV\)](#)

PhishDestroy Research Division

770,000+ threats tracked • 500,000+ domains blocked • 0.01% false-positive rate

[phishdestroy.io](#) • [Free Scanner](#) • [DestroyList](#) • [ScamIntelLogs](#)

© 2019-2026 PhishDestroy. CC BY 4.0 • PD-TRXDROP-2026-03-08